WHAT IS CLAIMED IS:

1. A method of authenticating memory devices' data within a gaming machine while said gaming machine is operating, said memory devices' data being authenticated substantially in parallel, said method of authenticating comprising:

reading a next predetermined amount of data from a first memory device;

if said next predetermined amount of data is graphic data, then reading a next predetermined amount of data;

if said next predetermined amount of data is executable code, then authenticating said executable code.

2. The method of claim 1, wherein the method of claim 1 is repeated substantially continuously while said gaming machine is operating.

3. The method of claim 1, wherein the method of claim 1 is repeated until said executable code cannot be authenticated.

4. The method of claim 1, wherein said next predetermined amount of data is a file.

5. The method of claim 1, wherein said first memory device is a volatile memory device containing a gaming machine program.

6. The method of claim 1, wherein if said next predetermined amount of data is said graphic data then determining whether a predetermined amount of events have passed, and wherein if said predetermined amount of events have passed then authenticating said graphic data.

7. The method of claim 1, further comprising: reading a next second-predetermined amount of data from a second memory device; and

determining whether said next-second predetermined amount of data is authentic;

repeating said reading said next second-predetermined amount of data step and said determining whether said next second-predetermined amount of data steps continuously while said gaming machine is operating, wherein said reading said next predetermined amount of data step and said reading said next second-predetermined amount of data is performed substantially in parallel.

8. The method of claim 1, further comprising

reading a next second-predetermined amount of data from a second memory device;

calculating a hash message digest with said next second-predetermined amount of data; and

determining whether all data from said second memory device has been read;

if all data from said second memory device has not been read then repeating said reading a next second-predetermined step, calculating step and determining whether steps again;

if all data from said second memory device has been read, then using said calculated hash message digest to authenticate the data in said second memory;

wherein said reading said next predetermined amount of data and said reading said next second-predetermined amount of data is performed substantially in parallel.

9. The method of claim 1, wherein authentication of said first and said second memory devices is performed repititiosly within a predetermined amount of time.

10. The method of claim 1 wherein said predetermined amount of time is an amount of time that is less than 24 hours.

11. In a gaming machine that is turned on, a method of repeatedly authenticating at least a first and a second memory substantially in parallel, said method comprising:

reading first data from said first memory and authenticating said first data, wherein reading first data from said first memory and authenticating said first data comprises:

reading a next file of said first data;

if said next file is a graphics data, then returning to said reading step;

if said next file is an executable code, then determining whether said executable file is authentic, then returning to said reading step until all of said first data in said first memory device has been read; and

reading second data from said second memory and authenticating said second data;

repeating said reading steps substantially continuously and substantially in parallel.

12. In said gaming machine, the method of claim 11, wherein reading said second data from said second memory and authenticating said second data comprises:

reading a next predetermined amount of data from said second data

using said next predetermined amount of data in a hash calculation;

determining if all of said second data has been read;

if all of said second data has not been read, then returning to said reading a next predetermined amount of data step;

if all of said second data has been read, then using said hash calculation to determine if said second data is authentic.

13. In said gaming machine, the method of claim 13, wherein said second memory is a high capacity storage memory.

14. In said gaming machine, the method of claim 11, wherein reading first data from said first memory and authenticating said first data comprises:

reading data in said first memory and performing a hash calculation on said read data, said hash calculation providing a result;

using said hash calculation result in a determination of whether said data from said first memory is authentic.

15. In said gaming machine, the method of claim 11, wherein reading first data from said first memory and authenticating said first data comprises;

reading data in said first memory and performing a CRC on said read data;

using said CRC to in a determination of whether said data from said first memory is authentic.

16. In said gaming machine, the method of claim 11, further comprising after said reading second data, reading third data from a third memory and authenticating said third data.

17. In said gaming machine, the method of claim 11, further comprising after said reading first data from said first memory, reading third data from a third memory and authenticating said third data in series with said reading first data from said first memory and authenticating said first data.

18. In said gaming machine, the method of claim 11, wherein each said reading steps are repeated at least once every predetermined amount of time.

19. In said gaming machine, the method of claim 12, wherein when said next file is said graphics data, then returning to said reading step unless a passing of a predetermined number of events has occurred; if said passing of said predetermined number of events has occurred then authenticating said graphics data.

20. A gaming machine comprising:

a user interface; and

a central processing unit (CPU) coupled to said user interface, said CPU comprising:

a processor;

a first memory coupled to said processor, said first memory adapted to contain gaming machine program code, said gaming machine program code comprising executable code and graphics data;

a second memory coupled to said processor, said second memory comprising data;

said gaming machine program code further comprises:

a plurality of instructions configured to cause said processor to determine the authenticity of said gaming machine program code and said data on a

substantially continuous, repetitious basis such that the authenticity determination of said gaming machine program code is performed substantially in parallel with the authenticity determination of said data;

said plurality of instructions are further configured to cause said processor to determine, when reading said gaming machine program code, whether said processor is reading executable code or graphics data,

if said processor reads graphics data, then said plurality of instructions cause said processor to not determine the authenticity of said graphics data unless more than a predetermined number of events have passed since the last time said graphics data was authenticated;

if said processor reads said executable code, then said plurality of instructions cause said processor to determine the authenticity of said executable code.

21. The gaming machine of claim 20, wherein said first memory is a volatile memory.

22. The gaming machine of claim 20, wherein said second memory is a non-volatile memory.

23. A gaming machine comprising

a CPU, and

a plurality of memory devices;

said CPU adapted to determine the authenticity of data in at least two of said plurality of memory devices in a parallel, repeating fashion;

said CPU further adapted to read said data stored in at least one of said plurality of memory devices and determine whether said data is executable code or graphics data;

if said data stored in said at least one of said plurality of memories is graphics data, then said CPU is adapted to determine the authenticity of said graphics data if a predetermined number of events have passed;

if said data stored in said at least one of said plurality of memories is executable code, then said CPU is adapted to determine the authenticity of said executable code.

24. The gaming machine of claim 23, wherein said predetermined number of events are measured in at least one of seconds, up counts, and down counts.

25. The gaming machine of claim 23, wherein said at least one of said plurality of memory devices that contains graphics data or executable code is a main memory.

26. The gaming machine of claim 25, wherein said graphics data and said executable code are both compiled data.

27. The gaming machine of claim 23, wherein said CPU is further adapted to determine the authenticity of other ones of said plurality of memory devices in a serial, repetitious fashion.

28. The gaming machine of claim 23, wherein said CPU is adapted to determine the authenticity of one, of said at least two of said plurality of memory devices, in a serial, repetitions manner with a plurality of other memory devices.

29. The gaming machine of claim 23, wherein said CPU is adapted to determine the authenticity of at least one of said plurality of memory devices using a hash calculation.

30. The gaming machine of claim 23, wherein said CPU is adapted to determine the authenticity of at least one of said plurality of memory devices using a CRC.

31. The gaming machine of claim 23, wherein said CPU is adapted to determine the authenticity of at least one of said plurality of memory devices by comparing a calculated signature with a stored signature.